

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of)
Kotaro KANEKO) Group Art Unit: Unassigned
Application No.: Unassigned) Examiner: Unassigned
Filed: August 26, 2003) Confirmation No.: Unassigned
For: CONTROLLING COMPUTER)
PROGRAM, CONTROLLING)
APPARATUS, AND CONTROLLING)
METHOD FOR DETECTING)
INFECTION BY COMPUTER VIRUS)

CLAIM FOR CONVENTION PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The benefit of the filing date of the following prior foreign application in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed:

Japan Patent Application No. 2003-092415

Filed: March 28, 2003

In support of this claim, enclosed is a certified copy of said prior foreign application. Said prior foreign application was referred to in the oath or declaration. Acknowledgment of receipt of the certified copy is requested.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By:

Platon N. Mandros
Registration No. 22,124

Date: August 26, 2003

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office

出願年月日

Date of Application: 2003年 3月28日

出願番号

Application Number: 特願2003-092415

[ST.10/C]:

[JP2003-092415]

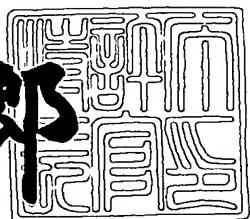
出願人

Applicant(s): ミノルタ株式会社

2003年 4月15日

特許庁長官
Commissioner,
Japan Patent Office

太田 信一郎



出証番号 出証特2003-3027024

【書類名】 特許願
【整理番号】 AK05412
【提出日】 平成15年 3月28日
【あて先】 特許庁長官 太田 信一郎 殿
【国際特許分類】 G06F 12/14
【発明の名称】 制御プログラムおよび制御装置
【請求項の数】 5
【発明者】
【住所又は居所】 東京都港区高輪二丁目16番29号 丸高高輪ビル 株式会社ミノルタソフトウェア研究所内
【氏名】 金子 巧太郎
【特許出願人】
【識別番号】 000006079
【氏名又は名称】 ミノルタ株式会社
【代理人】
【識別番号】 100072349
【弁理士】
【氏名又は名称】 八田 幹雄
【電話番号】 03-3230-4766
【選任した代理人】
【識別番号】 100102912
【弁理士】
【氏名又は名称】 野上 敦
【選任した代理人】
【識別番号】 100110995
【弁理士】
【氏名又は名称】 奈良 泰男
【選任した代理人】
【識別番号】 100111464

【弁理士】

【氏名又は名称】 齋藤 悅子

【選任した代理人】

【識別番号】 100114649

【弁理士】

【氏名又は名称】 宇谷 勝幸

【選任した代理人】

【識別番号】 100124615

【弁理士】

【氏名又は名称】 藤井 敏史

【手数料の表示】

【予納台帳番号】 001719

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 制御プログラムおよび制御装置

【特許請求の範囲】

【請求項1】 制御装置で用いられる制御プログラムであって、

前記制御装置による外部への通信の頻度を監視する手順と、

前記通信の頻度を予め設定されている閾値と比較することによって、前記制御装置でのコンピュータウイルスの感染を検知する手順と、をコンピュータに実行させることを特徴とする制御プログラム。

【請求項2】 前記通信の頻度を監視する手順では、複数の外部装置への通信の頻度が監視されることを特徴とする請求項1に記載の制御プログラム。

【請求項3】 前記通信の頻度を監視する手順では、特定の宛先ポートへ通信した頻度が監視されることを特徴とする請求項1に記載の制御プログラム。

【請求項4】 さらに、コンピュータウイルスの感染が検知された場合に、警告内容を前記制御装置が制御する画像形成装置に印刷させる手順をコンピュータに実行させることを特徴とする請求項1に記載の制御プログラム。

【請求項5】 制御装置であって、

当該制御装置による外部への通信の頻度を監視する監視手段と、

前記通信の頻度を予め設定されている閾値と比較することによって、当該制御装置でのコンピュータウイルスの感染を検知する検知手段と、を有することを特徴とする制御装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、制御プログラムおよび制御装置に関し、特に、コンピュータウイルスの感染を検知する制御プログラムおよび制御装置に関する。

【0002】

【従来の技術】

コンピュータウイルス（ただし、ワームも含む）の感染を検知し、コンピュータウイルスによる不正なプログラムおよびファイルを削除または隔離するための

種々の技術が知られている。

【0003】

たとえば、あるプログラムの正常時の動作仕様または典型動作を記憶しておき、この正常時の動作仕様または典型動作と、現状のプログラムの動作とを比較することによって、コンピュータウイルスの感染を検知する技術が知られている（たとえば、特許文献1参照）。またパーソナルコンピュータなどにおけるファイルサイズまたはリソースの変化からコンピュータウイルスの感染を検知する技術も知られている（たとえば、特許文献2参照）。

【0004】

また、近年では、多機能周辺機器（MFP：Multi-Function Peripheral）などの画像形成装置を制御するための制御装置として、画像形成装置専用に設計されたハードウェアを用いる代わりに、汎用のオペレーティングシステムが搭載されたパーソナルコンピュータを用いる技術が開発されている。このような場合、画像形成装置を制御するための制御装置がコンピュータウイルスに感染するおそれがある。

【0005】

しかしながら、従来の技術は、ウェブの閲覧、文章の作成、電子メールの送信、および表計算などの多様な用途に使用される汎用コンピュータにおけるコンピュータウイルスの感染に対処するためのものである。

【0006】

このため、従来の技術では、入出力されたファイルを監視し、そのファイル中にコンピュータウイルス特有の署名、形式、典型動作などを見つけ出すことで、コンピュータウイルスを検出するものが多い。このような技術では、コンピュータウイルスの感染を検知するためには、コンピュータウイルス特有の署名、形式、典型動作などを大規模なデータベースとして登録しておかなければならず、また、絶えず最新のデータベースに更新する必要があった。この結果、データベースの作成の作業負担が大きくなる。また、大規模なデータベースを用いて多量の比較処理を実行することが必要となるので、コンピュータウイルスを検出する際にCPUへ加わる負荷が増大して、コンピュータの処理能力が低下するおそれがあ

あった。

【0007】

特に、画像形成装置を制御するための制御装置のように用途が限定されている装置に対して、汎用コンピュータ用のコンピュータウイルス対策ソフトウェアを用いる場合には、C P Uへ加わる負荷の増大によって、画像形成装置の動作が遅延するおそれもあった。

【0008】

【特許文献1】

特開平9-171460号公報

【特許文献2】

特開平11-161517号公報

【0009】

【発明が解決しようとする課題】

本発明は、以上の問題点を解決するためになされたものである。したがって、本発明の目的は、コンピュータウイルスの感染を検知するためのデータベースの作成の作業負担を軽減することができる制御プログラムおよび制御装置を提供することである。さらに、本発明の目的は、コンピュータウイルスの感染を検知する際にC P Uに加えられる負荷を軽減することができる制御プログラムおよび制御装置を提供することである。

【0010】

また、本発明の他の目的は、画像形成装置を制御するための制御装置のように用途が限定されている装置においてコンピュータウイルスの感染の検知および対処を実行するために適した制御プログラムおよび制御装置を提供することである

【0011】

【課題を解決するための手段】

本発明の上記目的は、下記の手段によって達成される。

【0012】

(1) 本発明の制御プログラムは、制御装置で用いられる制御プログラムであ

って、前記制御装置による外部への通信の頻度を監視する手順と、前記通信の頻度を予め設定されている閾値と比較することによって、前記制御装置でのコンピュータウイルスの感染を検知する手順と、をコンピュータに実行させることを特徴とする。

【0013】

(2) 上記の通信の頻度を監視する手順では、複数の外部装置への通信の頻度が監視される。

【0014】

(3) 上記の通信の頻度を監視する手順では、特定の宛先ポートへ通信した頻度が監視される。

【0015】

(4) 上記の制御プログラムは、さらに、コンピュータウイルスの感染が検知された場合に、警告内容を前記制御装置が制御する画像形成装置に印刷させる手順をコンピュータに実行させる。

【0016】

(5) 本発明の制御装置は、当該制御装置による外部への通信の頻度を監視する監視手段と、前記通信の頻度を予め設定されている閾値と比較することによって、当該制御装置でのコンピュータウイルスの感染を検知する検知手段と、を有することを特徴とする。

【0017】

【発明の実施の形態】

以下、図面を参照して、本発明の実施の形態を説明する。

【0018】

図1は、本発明の一実施形態に係る制御装置としてのコンピュータが適用されたネットワークシステムの構成を示すブロック図である。

【0019】

図1に示すネットワークシステムは、多機能周辺機器(MFP: Multi-Function Peripheral)100を有している。MFP100は、制御装置として機能するコンピュータ200と、このコンピュータ200にケーブル500を介して接

続される複写機300とから構成されている。

【0020】

コンピュータ200は、たとえば、一般的なパーソナルコンピュータやワークステーションである。好ましくは、コンピュータ200には、汎用のオペレーティングシステム（OS）が搭載されており、複写機300と同一の筐体内に内蔵されている。すなわち、コンピュータ200は、複写機300などの画像形成装置を制御するために用途が限定されているものである。

【0021】

MFP100を構成するコンピュータ200は、ネットワーク600を介して、一般的なコンピュータであるクライアント400と相互に通信可能に接続されている。ネットワーク600は、イーサネット（登録商標）、トーカンリング、FDDI等の規格によるLANや、LAN同士を専用線で接続したWAN等からなる。なお、ネットワーク600に接続される機器の種類および台数は、図1に示される例に限定されない。

【0022】

MFP100は、複写機能に加えて、ネットワーク600を介して他の機器、たとえばクライアント400から受信したデータを複写機300で印刷するというネットワークプリンタとしての機能を有する。また、MFP100は、複写機300で原稿を読み取って得た画像データをネットワーク600を介して他の機器、たとえばクライアント400に送信するというネットワークスキャナとしての機能を有する。

【0023】

図2は、図1に示されるコンピュータ200の構成を示すブロック図である。図2に示すように、コンピュータ200は、装置全体の制御および各種演算処理を行うCPU201、プログラムやデータを格納するためのROM202、作業領域として一時的にプログラムやデータを記憶するためのRAM203、各種のプログラムやデータを保存するための外部記憶装置としてのハードディスク204、LANカードなどのネットワークインターフェース205、および複写機300にローカル接続するためのローカルインターフェース206を含み、これらは信

号を遺り取りするためのバス207を介して相互に接続されている。

【0024】

なお、コンピュータ200は、上述した構成要素以外の構成要素を含んでいてもよく、あるいは、上述した構成要素のうちの一部が含まれていなくてもよい。

【0025】

ハードディスク204には、オペレーティングシステムのほかに、ウイルススキャンプログラムがインストールされている。ウイルススキャンプログラムは、コンピュータウイルスの感染を検知し、不正なファイルや不正なプログラムを削除または隔離するための制御プログラムである。

【0026】

図3は、コンピュータ200にオペレーティングシステムおよびウイルススキャンプログラムがインストールされたときのプログラムおよびファイルの構成を概念的に示すブロック図である。これらのプログラムは、CPU201によって実行される。

【0027】

図3に示すように、プログラムおよびファイルは、目的とする機能によって、オペレーティングシステム210、ウイルススキャンプログラム220、およびプリントコントロール部230に大別される。

【0028】

オペレーティングシステム210は、一般的なオペレーティングシステムである。オペレーティングシステムのインストールに際して、外部への通信用のプログラム（たとえば、ブラウザやメールソフト）が付随してインストールされてもよい。

【0029】

プリントコントロール部230は、オペレーティングシステム210と共同して、MFP100への各ジョブの管理を行うプログラムである。

【0030】

ウイルススキャンプログラム220は、複数の機能モジュールを有する。具体的には、ウイルススキャンプログラム220には、パケットモニタ221、ファ

イルスキヤン222、起動プログラム状態スキヤン223、およびメッセージ出力224の各モジュールが含まれる。また、これらのモジュールに関連して、各種のパラメータを含む初期設定ファイル225と、データベース240とが設けられている。データベース240には、後述するファイルリスト241および起動プログラム状態リスト242がテーブル形式で記憶されている。また、後述するように不正なデータファイルやプログラムファイルを隔離するための隔離フォルダ226が用意されている。

【0031】

パケットモニタ221は、後述するパケットチェックおよびポートチェックをおこなうためのモジュールである。すなわち、パケットモニタ221によれば、コンピュータ200から外部への通信の頻度が監視されて、コンピュータ200でのコンピュータウイルスの感染が検知される。

【0032】

ファイルスキヤン222は、コンピュータ200内、特にハードディスク204上の論理ドライブ内の所定記憶領域に存在する各ファイルを確認し、存在が確認された各ファイルのなかで、ファイルリスト241に含まれていないファイルを、コンピュータウイルスに起因する不正なファイルと判断するためのモジュールである。なお、不正なファイルと判断されたファイルは削除または隔離フォルダ226内に隔離される。

【0033】

起動プログラム状態スキヤン223は、コンピュータ200内でCPU201によって実際に起動されている各プログラムを確認し、起動が確認された各プログラムのなかで、起動プログラム状態リスト242に含まれていないプログラムを、コンピュータウイルスに起因する不正なプログラムと判断するためのモジュールである。なお、不正なプログラムと判断されたプログラムは、削除または隔離フォルダ226内に隔離される。

【0034】

メッセージ出力224は、コンピュータ200でのコンピュータウイルスの感染が検知された場合に、コンピュータウイルスの感染を警告するための警告内容

を複写機300に印刷させるためのモジュールである。

【0035】

初期設定ファイル225は、各種のパラメータや閾値を予め設定するためのファイルである。また、パケットモニタ221、ファイルスキャン222、および起動プログラム状態スキャン223での処理範囲を特定するための情報も、初期設定ファイル225に含まれている。

【0036】

ファイルリスト241は、MFP100を制御するためにハードディスク204の論理ドライブ上の所定の記憶領域に存在することが必要な各ファイルの一覧である。ファイルリスト241には、各ファイルの名称およびその格納先のディレクトリ情報が含まれており、さらに各ファイルのサイズについての情報が含まれていてもよい。ファイルリスト241は、ファイルスキャン部222の処理で参照される。

【0037】

一方、起動プログラム状態リスト242は、MFP100を制御するために起動され得る各プログラムの一覧である。起動プログラム状態リスト242は、起動プログラム状態スキャン部223の処理で参照される。起動プログラム情報リスト242には、各プログラムの名称（各プログラムの実行ファイルの名称）およびその格納先のディレクトリ情報が含まれており、さらに各プログラムのサイズ（各プログラムの実行ファイルのサイズ）についての情報が含まれていてよい。

【0038】

なお、ファイルリスト241および起動プログラム状態リスト242は、MFP100などの出荷前に予め設定され、ハードディスク内に記憶されている。

【0039】

次に、図4～図5を参照して、以上のように構成される制御装置としてのコンピュータ200による処理について説明する。図4および図5のフローチャートに示されるアルゴリズムは、コンピュータ200のハードディスク204に記憶されており、CPU201によって実行される。

【0040】

なお、コンピュータ200による処理は、パケットモニタの処理と、ファイルスキャンおよび起動プログラム状態スキャンの処理とに大別される。図4および図5に示されるフローチャートのステップS101からステップ112までの処理がパケットモニタの処理に対応し、ステップS113からステップS119までの処理がファイルスキャンおよび起動プログラム状態スキャンの処理に対応する。

【0041】

(パケットモニタ処理)

まず、パケットモニタの処理について説明する。最初に、コンピュータ200のネットワークインターフェース205から出力されるパケットの情報が取得される（ステップS101）。一般に、コンピュータ200からの通信は、パケットと呼ばれるデータ伝送単位に分割されて行われる。パケットには、宛先IPアドレスおよび送信元IPアドレスが含まれるIPヘッダの部分、および宛先ポート番号および送信元ポート番号が含まれるTCPヘッダの部分が含まれている。ステップS101では、各パケットにおける宛先IPアドレスが抽出される。

【0042】

続いて、パケットの宛先、具体的には宛先IPアドレスがローカル（自分宛）であるか否かが判断される（ステップS102）。これによって、外部への通信か否かが判断される。パケットの宛先がローカルである場合には（ステップS102:YES）、ステップS101に戻って、パケットの監視が続行される。一方、パケットの宛先がローカルでなく、リモートである場合には（ステップS102:NO）、外部への通信であるとして、ステップS103へ進む。

【0043】

続いて、ステップS104およびステップS105に示されるポートチェックを前回行ってから所定時間（ポーリング時間）が経過しているか否かが判断される（ステップS103）。すなわち、ポートチェックは、一定時間毎に行われる。なお、ポートチェックを連続的に行わないで、ポーリング時間の経過を待って行うのは、ポートチェックを連続的に行うことによってコンピュータ200のC

PU201の負荷が高くなることを防止するためである。ポーリング時間が既に経過している場合には（ステップS103：YES）、ステップS104へ進み、ポートチェックの処理を実行する。

【0044】

まず、ポートチェックによる監視対象となる特定の宛先ポートと、第1閾値とが取得される（ステップS104）。なお、対象となる特定の宛先ポート、および第1閾値は、事前に設定されており、初期設定ファイル225に含まれている。

【0045】

具体的には、宛先ポートは、TCP/IPプロトコルで規定されている宛先ポート番号である。宛先ポート番号は、通信相手先のアプリケーションを識別するものであり、HTTPサーバへの通信の場合には80番となり、FTPサーバへの通信の場合には21番となる。

【0046】

続いて、SYN_SENDの数が監視される（ステップ105）。ここで、SYN_SENDとは、TCP/IPプロトコルにしたがってコンピュータ200が外部へ通信しようと試みることにより生じる状態を意味する。より具体的には、コンピュータ200から外部のコンピュータへの接続要求パケット（SYNパケットとも呼ばれる）の送信にともなって生じる状態を意味する。なお、SYN_SENDの状態は、時間の経過や状態の遷移によって消える。SYN_SENDが一時刻で発生している数は、オペレーティングシステム210に設けられた機能などを用いて監視することができる。実際には、特定の宛先ポート番号（本実施の形態では80番。尚、21番であってもよい）を持つ接続要求パケットの送信に伴って生じるSYN_SENDの数が監視される。

【0047】

続いて、確認されたSYN_SENDが一時刻で発生している数を第1閾値と比較する（ステップS106）。SYN_SENDが一時刻で発生している数が第1閾値を超えている場合には（ステップS106：YES）、コンピュータ200でのコンピュータウイルスの感染が検知され、後述するステップS115以

以下の処理によって、コンピュータウイルスに起因するプログラムが削除または隔離される。一方、SYN_SENDが一時刻で発生している数が第1閾値以下の場合には（ステップS106：NO）、この時点では、コンピュータウイルスの感染が確認されなかったと判断され、ステップS107の処理に進む。

【0048】

以上のステップS104～ステップS106に示されるポートチェックの処理においては、SYN_SENDの数に応じて、コンピュータウイルスの感染が検知される。

【0049】

一般に、通信を試みた相手先の数が多いほど、SYN_SENDの数が多くなる。また、存在しないIPアドレスや接続を確立できない相手先に対して通信を試みた場合にも、SYN_SENDは生じる。また、このような場合には、状態が遷移するまで時間がかかるので、SYN_SENDの状態が比較的長く継続する。

【0050】

典型的なコンピュータウイルスは、外部のサーバなどのコンピュータへの感染を図るために、無作為のIPアドレスへ通信を試みて、コンピュータウイルス自身を外部のコンピュータへ複製したり、脆弱性を攻撃したりする。したがって、コンピュータウイルスに感染した場合には、SYN_SENDが一時刻で発生している数が増加する。

【0051】

ここで、本実施の形態のコンピュータ200は、複写機300などの画像形成装置を制御するために用途が限定されており、ユーザによる操作や新規のプログラムの導入がなされない。したがって、このコンピュータ200は、外部のコンピュータへ接続要求パケットを送信する必要はなく、通信は、クライアント400側から接続要求パケットを受信することによって開始される。この結果、コンピュータウイルスに感染していない場合には、SYN_SENDが一時刻で発生している数が増加しない。したがって、SYN_SENDの数に応じて、コンピュータウイルスの感染の有無を判断することができる。

【0052】

次に、パケットチェックの処理について説明する。ステップS103で、ポーリング時間が未だ経過していない場合（ステップS103：NO）や、SYN_SENDの数が第1閾値以下である場合には（ステップS106：NO）、ステップS107に進む。

【0053】

まず、取得されたパケットの宛先ポート番号が、パケットチェックによる監視対象となる特定の宛先ポート（本実施の形態では80番である。尚、21番であってもよい）であるかが判断される（ステップS107）。なお、パケットチェックによる監視の対象となる特定の宛先ポートは、事前に設定されており、初期設定ファイル225に含まれている。パケットにおける宛先ポート番号が監視対象となる特定の宛先ポートでない場合には（ステップS107：NO）、このパケットをカウントアップすることなく、ステップS101に戻り、次のパケットの情報が取得される。一方、パケットにおける宛先ポート番号が監視対象となる特定の宛先ポートである場合には（ステップS107：YES）、送信されたパケットの数を数える（ステップS108）。この結果、特定の宛先ポート番号を持つパケットの送信の頻度が監視される。すなわち、単位時間あたりに送信されたパケットの数が監視される。

【0054】

次に、特定の宛先ポート番号を持つパケットの送信の頻度が第2閾値と比較される（ステップS109）。なお、第2閾値は、事前に設定されており、初期設定ファイル225に含まれている。送信の頻度が第2閾値を超えている場合には（ステップS109：YES）、コンピュータ200がコンピュータウイルスに感染しているおそれがある。したがって、ポーリング時間が経過しているか否かにかかわらず、ポートチェックの処理（ステップS110～ステップS112）を隨時に実行する。一方、送信の頻度が第2閾値以下である場合には（ステップS109：NO）、ステップS101の処理に戻る。なお、ステップS110～ステップS112のポートチェックの処理は、上述したステップS104～ステップS106の処理と同様であるので、詳しい説明を省略する。

【0055】

以上のとおり、本実施の形態では、コンピュータ200による外部への通信の頻度を監視し、通信の頻度を予め設定されている閾値と比較することによって、コンピュータウイルスの感染を検知する。複数の外部装置（たとえば、Webサーバなど）への通信の頻度が監視され、より具体的には、特定の宛先ポートへ通信した頻度が監視される。

【0056】

本実施の形態では、コンピュータ200による外部への通信の頻度を監視する方法として、ポートチェック（ステップS104～ステップS106、およびステップS110～ステップS112を参照）と、パケットチェック（ステップS107～ステップS109）の双方を用いている。ポートチェックでは、特定の宛先ポート番号をもつ接続要求パケット（SYNパケット）の送信の頻度が監視される。特に、接続要求パケットの送信に伴って生じる状態であるSYN_SEN Dが一時刻で発生している数を監視することで、複数のサーバなどへの通信した頻度が監視できる。一方、パケットチェックでは、特定の宛先ポート番号を持つパケットを単位時間あたりに送信した数が監視される。

【0057】

ポートチェックの処理では、コンピュータウイルスの感染の有無による違いが明確なSYN_SEN Dの数を基準に、感染の有無を判断するため、第1閾値の設定が容易であり、感染の有無を最終的に確定する処理に特に適するという長所を有する。しかしながら、ポートチェックの処理では、パケットチェックの処理に比べて、CPU201へ与える負荷が高い。また、SYN_SEN Dの状態が消えるタイミングとポーリング時間との関係によっては、SYN_SEN Dの数の増加を確認できないおそれがある。

【0058】

一方、パケットチェックの処理では、ポートチェックの場合と比べて、CPU201の処理能力に与える影響が小さいので、一定時間ごとではなく常に実行することが容易である。また、ポートチェックの場合と異なり、実行するタイミングによらず、パケットの送信の頻度増加を確認しやすい。しかしながら、クライ

アント400から多量のデータを受信して複写機300で印刷する場合のように、コンピュータウイルスに感染していないにもかかわらず、パケットの送信の頻度が高くなるおそれがある。したがって、第2閾値の設定が難しい場合がある。

【0059】

したがって、図4に示されたように、ポートチェックの処理とパケットチェックの処理とを併用して実行することによって、それぞれの特徴を生かして、CPU201への負荷を高めることなく、確実にコンピュータウイルスの感染の有無を判断することができる。

【0060】

しかしながら、本実施の形態と異なり、パケットチェックまたはポートチェックのどちらか一方を用いて、コンピュータ200から外部への通信の頻度を監視して、コンピュータ200でのコンピュータウイルスの感染を検知してもよい。

【0061】

(ファイルスキャンおよび起動プログラム状態スキャンの処理)

次に、コンピュータ200がコンピュータウイルスに感染していると判断された場合の処理を説明する。本実施の形態では、この場合、ファイルスキャンおよび起動プログラム状態スキャンの処理が実行される。

【0062】

まず、ステップS113～ステップS116に示されるファイルスキャンの処理について説明する。

【0063】

ファイルスキャンの処理の前提として、ファイルリスト241、すなわち、MFP100を制御するためにコンピュータ200内のハードディスク204の論理ドライブ上の所定の記憶領域（所定のディレクトリ）に存在する必要がある各ファイルの一覧を予め設定し記憶する処理がなされる。MFP100を制御するために必要な各ファイルには、たとえば、オペレーティングシステムおよびプリントコントロールに対応するファイルが該当する。具体的には、コンピュータ200がコンピュータウイルスに感染していない状態で、ファイルリスト241が設定され、記憶される。

【0064】

次に、実際の処理では、初期設定ファイル225を参照して、監視対象となる所定の記憶領域についての情報を取得する（ステップS113）。具体的には、ハードディスク204の論理ドライブ上での所定のディレクトリが所定の記憶領域として予め設定されている。したがて、ステップS113では、たとえば、所定のディレクトリを指定するための情報が取得される。そして、この所定のディレクトリに存在する各ファイルが確認される。さらに、ファイルの拡張子などを用いて、所定の記憶領域をより詳細に指定しておいてもよい。なお、MPF100が印刷ジョブなどを実行する際に印刷データのファイルなどを一時的に記憶するためのディレクトリなどは、所定の記憶領域となるディレクトリからは、除外しておくことが望ましい。

【0065】

続いて、コンピュータ200内のハードディスク204の所定の記憶領域に実際に存在する各ファイルが確認される（ステップS114）。具体的には、指定された所定の記憶領域に対応するディレクトリにある各ファイルの名称が確認される。また、各ファイルのサイズについて確認してもよい。

【0066】

続いて、ステップS114で確認されたファイルのなかで、ファイルリスト241に含まれていないファイルがあるか否かが判断される（ステップS115）。具体的には、ステップS114で確認された各ファイルの名称とファイルリスト241に含まれている各ファイルの名称とが比較される。また、ステップS114で確認された各ファイルのサイズと、ファイルリスト241に含まれている各ファイルのサイズとが比較されてもよい。

【0067】

比較の結果、ステップS114で確認されたファイルの中に、ファイルリスト241に含まれていないファイルがある場合（ステップS115：YES）、このファイルリスト241に含まれていないファイルをコンピュータウイルスに起因する不正なファイルと判断し、ステップS116の処理に進む。一方、ステップS114で確認されたファイルのすべてが、ファイルリスト241に含まれて

いる場合（ステップS115：NO）、ステップS120の処理に進む。

【0068】

続いて、不正なファイルと判断されたファイルが削除され、または、隔離フォルダ226内へ隔離される（ステップS116）。

【0069】

コンピュータウイルスがコンピュータ200内に侵入した場合、コンピュータウイルスによって新たなファイルが作られることが多い。以上のステップS113～ステップS116に示されるファイルスキャンの処理は、このような症状を検出して、コンピュータウイルスが原因で出現したファイルを見つけ出して除去するものである。

【0070】

ここで、コンピュータ200は、複写機300などの画像形成装置を制御するための制御装置であり、用途が限定されている。したがって、汎用の場合と異なり、ユーザが新規のファイルを作成し、あるいはソフトウェアをインストールするような操作が行われにくい。特に、コンピュータ200が複写機300の同一筐体内に内蔵されている場合には、この傾向が強い。

【0071】

したがって、画像形成装置の制御に必要なファイルリストを作成しておき、このファイルリストに含まれていない新規のファイルが出現した場合は、このファイルはコンピュータウイルスに起因して作成されたものであると判断することができる。このように、用途が限定されているコンピュータ200に対して、ファイルスキャンの処理を適用することで、効率的にコンピュータウイルスに感染したファイルを除去または隔離することができる。

【0072】

次に、ステップS117～ステップS119に示される起動プログラム状態スキャンの処理について説明する。

【0073】

起動プログラム状態スキャンの処理の前提として、起動プログラム状態スキャンリスト242、すなわち、MFP100を制御するために起動され得る各プロ

グラムの一覧を予め設定し記憶する処理がなされる。MFP100を制御するために起動され得るプログラムには、たとえば、オペレーティングシステムおよびプリントコントロールに対応するプログラムが含まれる。具体的には、コンピュータ200がコンピュータウイルスに感染していない状態で、起動プログラム状態リスト242が設定され、記憶される。

【0074】

まず、コンピュータ200内でCPU201によって実際に起動されている状態にあるプログラムが確認される（ステップS117）。たとえば、オペレーティングシステム210が有する機能を用いて、実際に起動されている状態にあるプログラムが確認される。この結果、実際に起動されている状態にあるすべてのプログラムをリストアップされた状態で確認することができる。具体的には、起動されている状態にあるプログラムの名称やサイズが確認される。

【0075】

続いて、ステップS117で起動が確認されたプログラムのなかで、起動プログラム状態リスト242に含まれていないプログラムがあるか否かが判断される（ステップS118）。具体的には、起動が確認された各プログラムの名称と、起動プログラム状態リスト242に含まれている各プログラムの名称とが比較される。また、起動が確認された各プログラムのサイズと、起動プログラム状態リスト242の各プログラムのサイズとが比較されてもよい。

【0076】

比較の結果、ステップS117で起動が確認されたプログラムの中に、起動プログラム状態リスト242に含まれていないプログラムがある場合（ステップS118：YES）、この起動プログラム状態リスト242に含まれていないプログラムをコンピュータウイルスによる不正なプログラムであると判断し、ステップS119の処理へ進む。一方、ステップS117で起動が確認されたプログラムのすべてが、起動プログラム状態リスト242に含まれている場合（ステップS118：NO）、ステップS120の処理に進む。

【0077】

続いて、不正なプログラムと判断されたプログラムの実行形式のプログラムフ

イルを削除し、または、隔離フォルダ226内へ隔離する（ステップS119）。

【0078】

コンピュータウイルスがコンピュータ200内に侵入した場合、コンピュータウイルスによって、画像形成装置の制御に無関係なプログラムが実行されることが多い。以上のステップS117～ステップS119に示される起動プログラム状態スキャンの処理は、このような症状を検出して、コンピュータウイルスが原因で実行されたプログラムを見つけ出し、そのプログラムファイルを除去したり、待避したりするものである。

【0079】

ここで、コンピュータ200は、複写機300などの画像形成装置を制御するための制御装置であり、用途が限定されている。したがって、汎用の場合と異なり、画像形成装置の制御に無関係なプログラムを実行させる操作がユーザによって行われない。特に、コンピュータ200が複写機300の同一筐体内に内蔵されている場合には、この傾向が強い。

【0080】

したがって、画像形成装置を制御するために起動され得るプログラムのリストである起動プログラム状態リストを作成しておき、この起動プログラム状態リストに含まれていないプログラムの起動状態が出現した場合には、このプログラムはコンピュータウイルス自体か、あるいはコンピュータウイルスに起因して実行されているプログラムであると判断することができる。このように、用途が限定されているコンピュータ200に対して、起動プログラム状態スキャンの処理を適用することで、効率的にコンピュータウイルスまたはコンピュータウイルスに感染したプログラムを除去または隔離することができる。

【0081】

最後に、コンピュータウイルスに感染したことを警告するための印刷処理について説明する。換言すれば、この印刷処理は、コンピュータウイルスの感染が検知された場合に、警告内容を、コンピュータ200が制御するMFPに印刷させる処理である。

【0082】

図5のステップS120に示されているように、コンピュータ200がコンピュータウイルスに感染していると判断された場合には、コンピュータ200は、複写機300にウイルスに感染している旨の判断結果を印刷させる。換言すれば、MFP100は、制御装置として自己に内蔵されているコンピュータ200がコンピュータウイルスに感染している旨のメッセージを有する警告文書を自らの印刷機能を用いて印刷することができる。

【0083】

図6に印刷される警告内容の例を示す。なお、警告内容は、たとえば、事前にハードディスク204内に記憶されている画像データに基づいて印刷される。

【0084】

なお、上述した例では、ファイルスキャンの処理（ステップS113～ステップS116）を実行した後に、起動プログラム状態スキャン（ステップS117～ステップS119）を実行する場合を説明したが、ファイルスキャンの処理と、起動プログラム状態スキャンの処理とを実行する順番は、この場合に限られない。

【0085】

また、上述した例では、ポートチェック（ステップS104～ステップS106、およびステップS110～ステップS112）、および／またはパケットチェック（ステップS107～ステップS109）によって、コンピュータ200でのコンピュータウイルスの感染が明らかになった場合に限って、ファイルスキャンの処理、および起動プログラム状態スキャンの処理を実行する場合を説明した。このような構成を採用したのは、ファイルスキャンの処理および起動プログラム状態スキャンの処理が、パケットチェックの処理に比べてCPU201に与える負荷が高いことに起因する。すなわち、ファイルスキャンの処理および起動プログラム状態スキャンの処理を定常的に行うこと回避して、CPU201がMFP100を制御する際の処理能力への影響を小さくしている。

【0086】

しかしながら、ポートチェック、およびパケットチェックと無関係に、ファイ

ルスキヤンの処理および／または起動プログラム状態スキャンの処理を実行することも可能である。また、ポートチェック、および／またはパケットチェックにより、コンピュータ200でのコンピュータウイルスの感染が明らかになった場合に、ファイルスキャンの処理および／または起動プログラム状態スキャン以外の処理を行うこともできる。たとえば、コンピュータウイルスの感染が明らかになった場合に、警告のみを行ってもよい。

【0087】

以上の説明では、制御装置として、MFP100を制御するためのコンピュータ200を例にとって示したが、本発明はこの場合に限られない。種々の制御装置に対して、本発明を適用することができる。

【0088】

本発明において、制御装置における各種処理を行う手段は、専用のハードウェア回路、またはプログラムされたコンピュータのいずれによっても実現することが可能である。上記プログラムは、例えばフレキシブルディスクやCD-ROMなどのコンピュータ読み取り可能な記録媒体によって提供されてもよいし、インターネット等のネットワークを介してオンラインで提供されてもよい。この場合、コンピュータ読み取り可能な記録媒体に記録されたプログラムは、通常、ハードディスク等の記憶部に転送されて記憶される。また、上記プログラムは、単独のアプリケーションソフトとして提供されてもよいし、装置の一機能としてその装置のソフトウェアに組み込まれてもよい。

【0089】

以上のように本発明の好適な実施の形態を説明したが、本発明の技術的思想を逸脱しない範囲内において、当業者が種々の変更、追加、および省略をすることができるることは明らかである。

【0090】

なお、上述した本発明の実施形態には、特許請求の範囲の請求項1～5に記載した発明以外にも、以下の付記1～28に示すような発明が含まれる。

【0091】

【付記1】 前記通信の頻度を監視する手順では、パケットを単位時間あたり

に送信した数が監視されることを特徴とする請求項1に記載の制御プログラム。

【0092】

[付記2] 前記通信の頻度を監視する手順では、特定の宛先ポート番号をもつパケットを単位時間あたりに送信した数が監視されることを特徴とする付記1に記載の制御プログラム。

【0093】

[付記3] 前記特定の宛先ポート番号は、H T T P サーバへ送信する際に用いられるポート番号であることを特徴とする付記2に記載の制御プログラム。

【0094】

[付記4] 前記特定の宛先ポート番号は、F T P サーバへ送信する際に用いられるポート番号であることを特徴とする付記2に記載の制御プログラム。

【0095】

[付記5] 前記通信の頻度を監視する手順では、接続要求パケットを送信した頻度が監視されることを特徴とする請求項1に記載の制御プログラム。

【0096】

[付記6] 前記通信の頻度を監視する手順では、特定の宛先ポート番号をもつ接続要求パケットを送信した頻度が監視されることを特徴とする請求項1に記載の制御プログラム。

【0097】

[付記7] 接続要求パケットを送信した頻度として、接続要求パケットの送信に伴って生じる状態が一時刻で発生している数が監視されることを特徴とする付記5または付記6に記載の制御プログラム。

【0098】

[付記8] 接続要求パケットを送信した頻度として、接続要求パケットの送信に伴って生じるS Y N _ S E N D が一時刻で発生している数が監視されることを特徴とする付記5または付記6に記載の制御プログラム

[付記9] 前記特定の宛先ポート番号は、H T T P サーバへ送信する際に用いられるポート番号であることを特徴とする付記6に記載の制御プログラム。

【0099】

[付記10] 前記特定の宛先ポート番号は、FTPサーバへ送信する際に用いられるポート番号であることを特徴とする付記6に記載の制御プログラム。

【0100】

[付記11] 前記通信の頻度を監視する手順をコンピュータに所定時間ごとに繰り返えし実行させることを特徴とする請求項1に記載の制御プログラム。

【0101】

[付記12] 前記通信の頻度を監視する手順では、パケットを単位時間あたりに送信した数が監視されるとともに、特定の宛先ポート番号をもつ接続要求パケットの送信に伴って生じる状態が一時刻で発生している数が監視されることを特徴とする請求項1に記載の制御プログラム。

【0102】

[付記13] 前記通信の頻度を監視する手順では、パケットを単位時間あたりに送信した数が監視されるとともに、特定の宛先ポート番号をもつ接続要求パケットの送信に伴って生じるS Y N _ S E N Dが一時刻で発生している数が監視されることを特徴とする請求項1に記載の制御プログラム。

【0103】

[付記14] 前記制御装置は、画像形成装置を制御する装置であることを特徴とする請求項1に記載の制御プログラム。

【0104】

[付記15] 前記制御装置は、オペレーティングシステムが組み込まれたコンピュータであって、前記画像形成装置と同一の筐体内に内蔵されていることを特徴とする付記14に記載の制御プログラム。

【0105】

[付記16] 請求項1乃至請求項4、または付記1乃至付記15のいずれか一つに記載の制御プログラムを記録したコンピュータ読み取り可能な記録媒体。

【0106】

[付記17] 前記監視手段は、複数の外部装置への通信の頻度を監視することを特徴とする請求項5に記載の制御装置。

【0107】

[付記18] 前記監視手段は、特定の宛先ポートへ通信した頻度を監視することを特徴とする請求項5に記載の制御装置。

【0108】

[付記19] さらに、コンピュータウイルスの感染が検知された場合に、警告内容を前記制御装置が制御する画像形成装置に印刷させる印刷指示手段を有することを特徴とする請求項5に記載の制御装置。

【0109】

[付記20] 前記監視手段は、パケットを単位時間あたりに送信した数を監視することを特徴とする請求項5に記載の制御装置。

【0110】

[付記21] 前記監視手段は、特定の宛先ポート番号をもつパケットを単位時間あたりに送信した数を監視することを特徴とする付記20に記載の制御装置。

【0111】

[付記22] 前記監視手段は、接続要求パケットを送信した頻度を監視することを特徴とする請求項5に記載の制御装置。

【0112】

[付記23] 前記監視手段は、特定の宛先ポート番号をもつ接続要求パケットを送信した頻度を監視することを特徴とする請求項5に記載の制御装置。

【0113】

[付記24] 前記監視手段は、パケットを単位時間あたりに送信した数を監視するとともに、特定の宛先ポート番号をもつ接続要求パケットの送信に伴って生じる状態が一時刻で発生している数を監視することを特徴とする請求項5に記載の制御装置。

【0114】

[付記25] 前記監視手段は、パケットを単位時間あたりに送信した数を監視するとともに、特定の宛先ポート番号をもつ接続要求パケットの送信に伴って生じるSYN_SEN Dが一時刻で発生している数を監視することを特徴とする請

求項5に記載の制御装置。

【0115】

[付記26] 画像形成装置を制御する装置であることを特徴とする請求項5に記載の制御装置。

【0116】

[付記27] 前記制御装置は、オペレーティングシステムが組み込まれたコンピュータであって、前記画像形成装置と同一の筐体内に内蔵されることを特徴とする付記26に記載の制御装置。

【0117】

[付記28] 制御方法であって、制御装置による外部への通信の頻度を監視するステップと、前記通信の頻度を予め設定されている閾値と比較することによって、前記制御装置でのコンピュータウイルスの感染を検知するステップと、を有することを特徴とする制御方法。

【0118】

【発明の効果】

上述したように、本発明によれば、コンピュータウイルスを検出するためのデータベースの作成の作業負担を軽減し、コンピュータウイルスの検出処理の際ににおける負荷を軽減することができる制御プログラムおよび制御装置を提供することができる。特に、画像形成装置を制御するための制御装置のように用途が限定されている装置に適したコンピュータウイルス対処機能を有する制御プログラムおよび制御装置を提供することができる。

【図面の簡単な説明】

【図1】 本発明の一実施形態に係る制御装置としてのコンピュータが適用されたネットワークシステムの構成を示すブロック図である。

【図2】 図1に示されるコンピュータの構成を示すブロック図である。

【図3】 図1に示されるコンピュータ内のプログラムおよびファイルの構成を概念的に示すブロック図である。

【図4】 図1に示されるコンピュータの処理について説明するためのメインフローチャートである。

【図5】 図4に後続するフローチャートである。

【図6】 図1に示される複写機によって印刷される警告文書の例である。

【符号の説明】

100…MFP、

200…コンピュータ

201…CPU、

202…ROM、

203…RAM、

204…ハードディスク、

205…ネットワークインターフェース、

206…ローカルインターフェース、

210…オペレーティングシステム、

220…ウイルススキャンプログラム、

221…パケットモニタ、

222…ファイルスキャン、

223…起動プログラム状態スキャン、

224…メッセージ出力、

225…初期設定ファイル、

230…プリントコントロール部、

240…データベース、

241…ファイルリスト、

242…起動プログラム状態リスト

300…複写機、

400…クライアント、

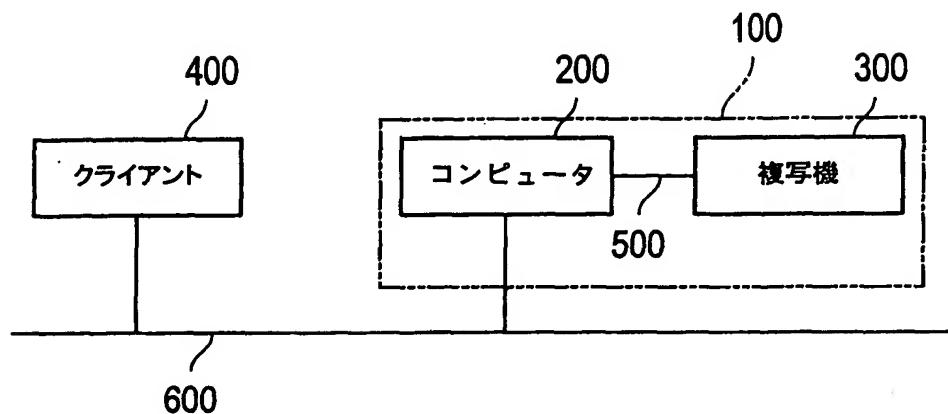
500…ケーブル、

600…ネットワーク。

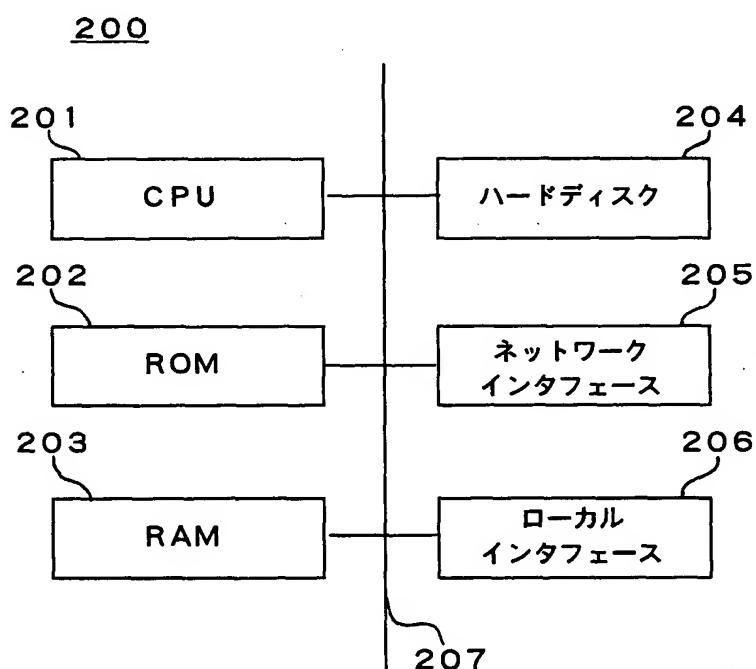
【書類名】

図面

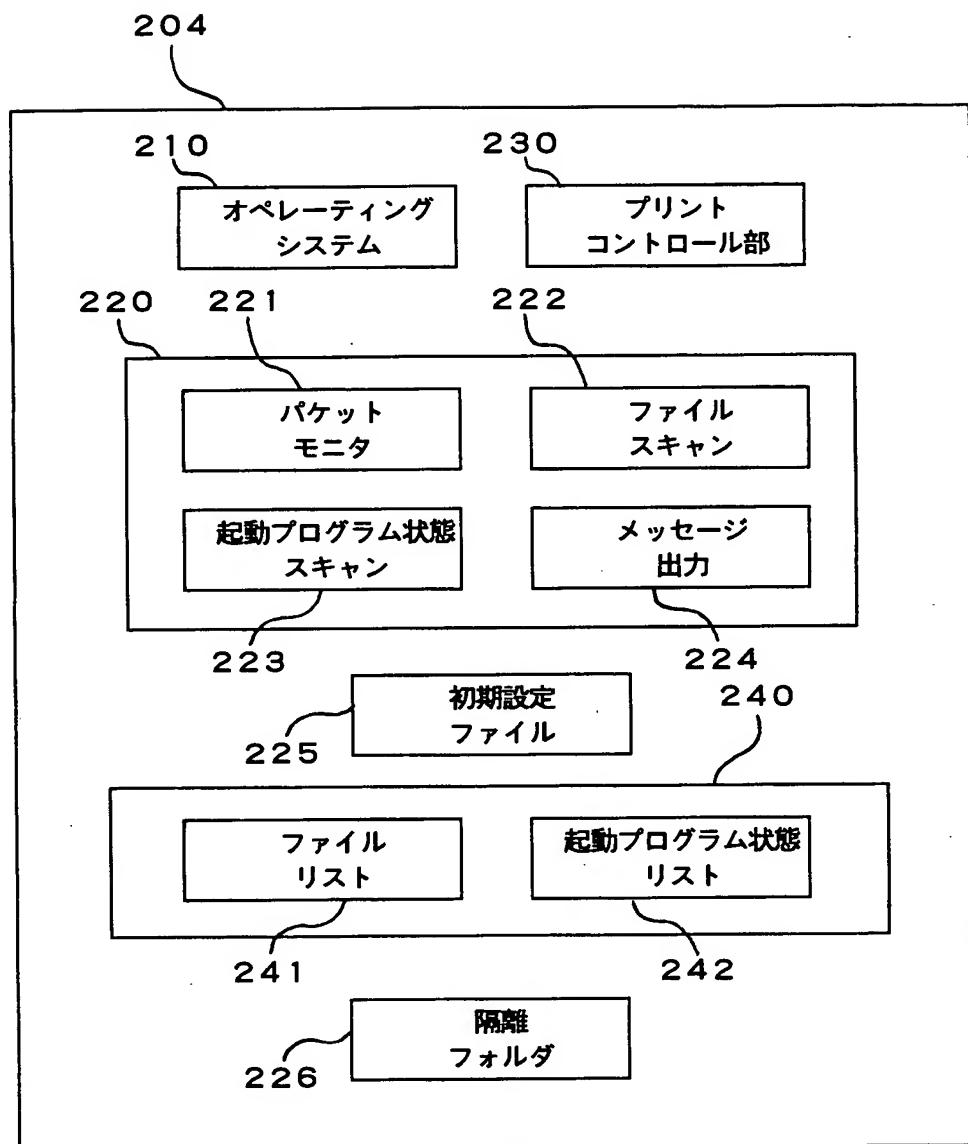
【図1】



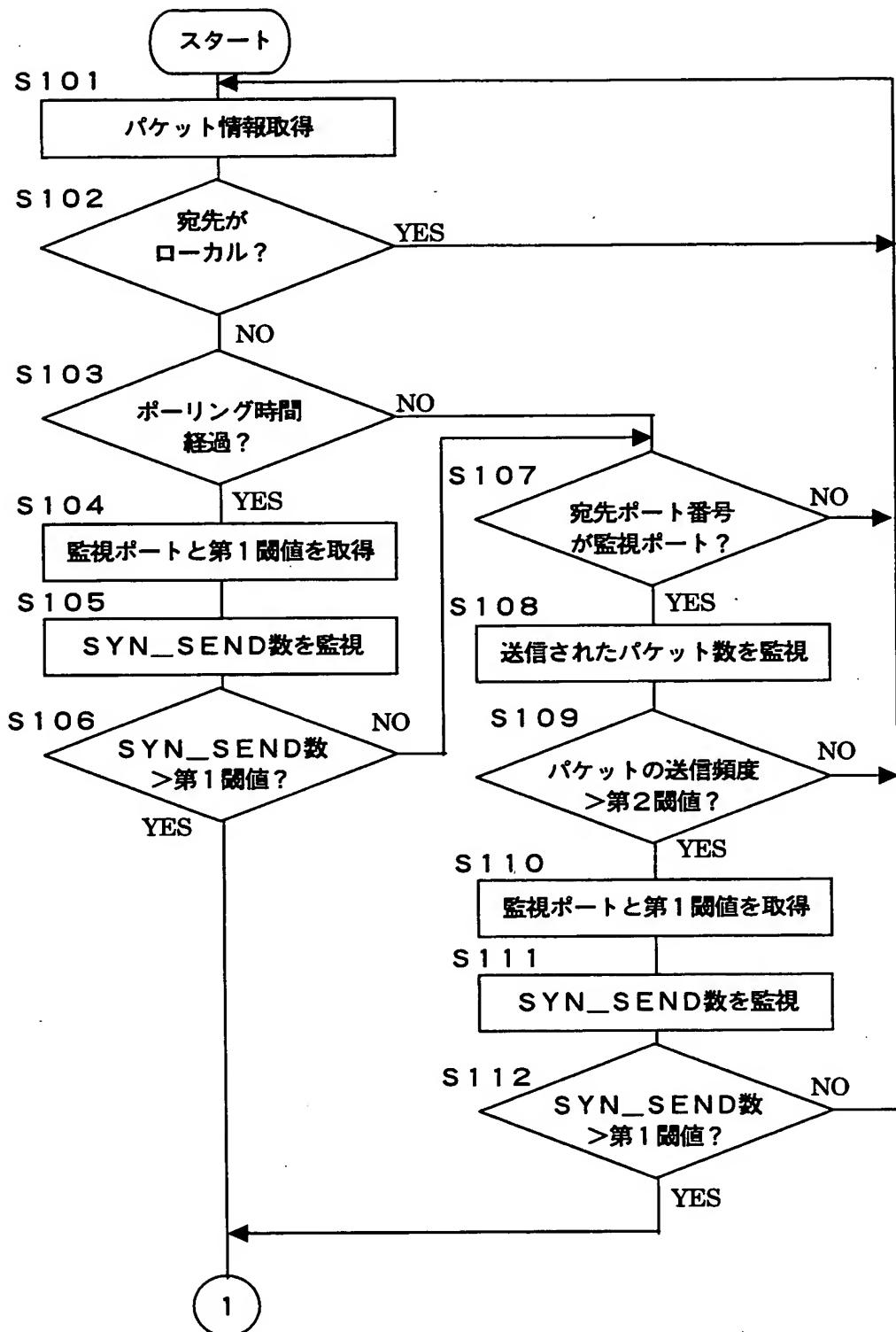
【図2】



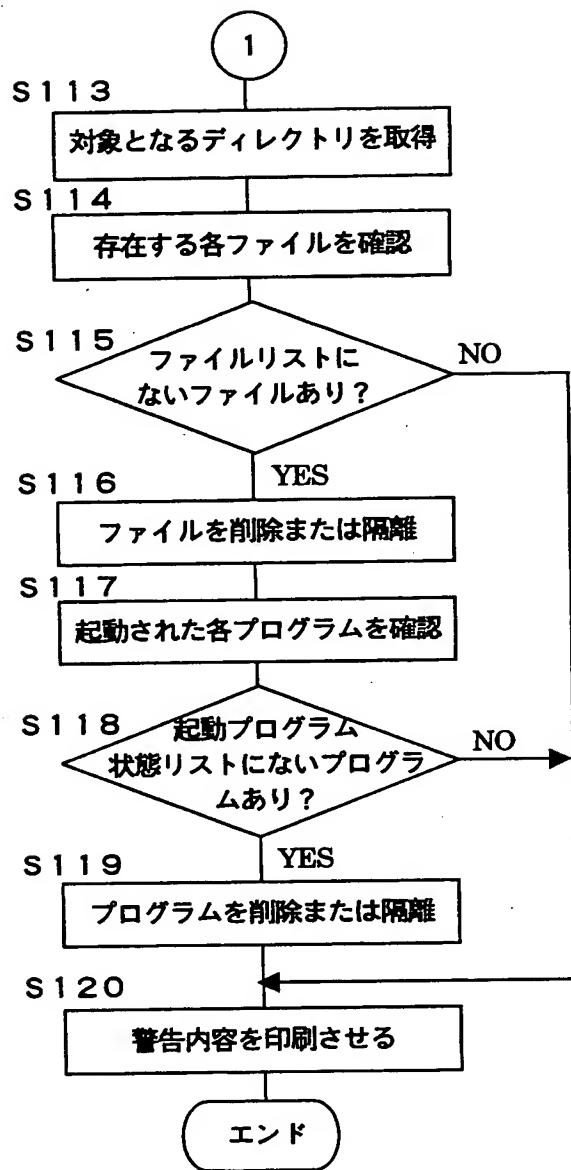
【図3】



【図4】



【図5】



【図6】

Warning!!

An illegal request was detected.
This device might be infected with the virus.
Please contact customer service.
9999-9999-9999

【書類名】 要約書

【要約】

【課題】 コンピュータウイルスの感染を検知するためのデータベースの作成の作業負担を軽減し、コンピュータウイルの感染を検知する際ににおける、負荷を軽減する。

【解決手段】 MFP100を制御するコンピュータ200は、コンピュータ200による外部への通信の頻度を監視し、通信の頻度を予め設定されている値と比較して、コンピュータ200がコンピュータウイルスに感染しているか否かを判断する。

【選択図】 図1

出願人履歴情報

識別番号 [000006079]

1. 変更年月日 1994年 7月20日

[変更理由] 名称変更

住所 大阪府大阪市中央区安土町二丁目3番13号 大阪国際ビル
氏名 ミノルタ株式会社